Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 11 (2013) 51 – 56

Procedia Technology

The 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013)

Rapid Encryption Method Based on AES Algorithm for Grey Scale HD Image Encryption

Salim M. Wadi[a,b]*, Nasharuddin Zainal[a]

[a]*Dept. of EE&S Eng., Faculty of Engineering and Built Environment,Universiti Kebangsaan Malaysia,UKM Bangi, Selangor 43600, Malaysia*
[b]*Com. Eng. Dep., Najaf Technical College, Foundation of Technical Education, South Street, Najaf 472, Iraq.*

Abstract

Ciphering is very important operation to preserve the confidentiality of digital images transmitted over public network spatially with rapidly growth in communication techniques. Advanced Encryption Standard (AES) is a famous and strong encryption algorithm which has several advantages in data ciphering. However, AES suffer from some drawbacks such as high computations, pattern in ciphered images, and hardware requirement. Those problems are more complicated when AES algorithm willusefor images ciphering especially the HD images. Some modifications were proposed in this paper to enhance the performance of AES algorithm in terms of time ciphering and pattern appearance. First modification is decreasing the number of rounds to one while the second modification is replace the S-box with new S-box to decrease the hardware requirements. Applying AES in one of the ciphering mode solves the pattern appearance problems. The experimental results indicate that the proposed modifications make AES algorithm faster while fulfill the security requirements.

*Keywords:*Image ciphering; AES algorithm; AES version; pattern appearance; mode encryption.

1. Introduction

Rapid evolution in communication systems such as satellite, mobile network, internet, earth communications, etc. make important to protect and preserve sensitive and critical public, private, and national infrastructures and their

* Corresponding author. Tel.: +60123974558.
E-mail address: salim2007555@yahoo.com, salimmw@eng.ukm.my

doi:10.1016/j.protcy.2013.12.161

respected data against attacker and illegal copying and distribution [1]. Encryption algorithm is best method used to keeping the information security. Encryption algorithms change the information into an inapprehensible form. Image encryption does on image pixels by change pixels locations (confusion) or pixels values (diffusion) where good ciphering if image ciphered form similar for Jamming form in TV. One of the public cryptography and widely used in large number of applications such as smart card, cell phone, automated teller machines, and www servers is the Advanced Encryption Standard (AES) [2]. The National Institute of Standard and Technology (NIST) accepted Advance Encryption Standard (AES) that produced by Rijndael in 2001. However, AES suffer from some drawbacks such as, long encryption and decryption time, and patterns appearance in the ciphered image [3].

Huang et al. [4] and Telagarapu et al. [5] used image compression to decrease the size of image and prevent the pattern appearance. A dynamic bit-width adaptation scheme in discrete cosine transforms (DCT) technique used for image compression. Kamali et al. [6] and Telagarapu et al. [5] proposed modification of AES algorithm by adjusting the ShiftRow Transformation. In this modification, two rows will be shifted with respect to three initial ASE depending on parity of 1'st element of state. Subramanyan et al. [7] and Muhaya and Fahad [8] used Chaotic Henon map to generate the key for AES algorithm. S-box substitution and add round key steps were used only by [7] after key generating. Muhaya and Fahad in [8] suggested shuffle the image pixels using Arnold's cat map and used Chaotic Henon map to key generation then apply AES algorithm. Tran et al. [9] and Chen et al. [10] modified the AES algorithm through S-box Modification. New S-box called Gray S-box is suggested by [9] to use in AES algorithm where the security of Gray S-box increased because it corresponded to a polynomial with all 255 non-zero terms in comparison with 9-term polynomial of original AES S-box. Whereas, fixed S-box replaced by inhomogeneous S-box which selected randomly is new modification to AES proposed by [10]. Jing et al [11] presented three types of MixColumn polynomials that can be easily provided diversified selections of the AES algorithm. The authors presented and discussed some properties of MixColumn and InvMixColumn polynomials to dive the user diversified selections.

This paper organized as follows, in Section 2 explanation to initial AES algorithm and new version is presented. The details of proposed modifications are introduced in Section 3. Statistical and computational aspects are shown in Section 4 and conclusions of this paper in Section 5.

2. Initial AES algorithm and modified version

2.1. AES algorithm

The AES developed by Joan Daemen and Vincent Rijmen has been selected by NIST as standard ciphering algorithm in 2002[12].There are three versions of AES algorithm depending on length of the key (AES128, AES192, and AES 256)bit and 128 bit block data which constructed in 4x4 matrix called state[13]. AES algorithm is divided into four sequential operations; where these operations are made on a state with (10, 12, 14) rounds based on key length. The first transformation is SubBytewhich is nonlinearly substitute the state bytes independently using substitution table (S-box)[12]. Shift row operation is second transformation apply on state rows where, 1st row no shifted, 2nd row shifted to right one time, 3rd row shifted to right two times, and 4th row shifted to right three times. The third transformation is Mixcolumn transformation which carries out on state column by column. Each byte is replaced by a value dependent on all 4 bytes in same column through multiplication state matrix in GF(2^8) as in Eq. (2) and using Eq. (1) [13]:

$$m(x) = x^8 + x^4 + x^3 + x + 1 \tag{1}$$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix} \tag{2}$$

Lastly is the Add Round Key transformation which is a simple bitwise XOR between 16 byte state matrix and a portion of the expanded key (16 byte key matrix) for more details about AES algorithm see [12].

2.2. Modified AES algorithm

One problem in AES algorithm is patterns appearance in the ciphered image due to the presence a region with similar colour in original image. New modification for AES algorithm was proposed in[6]. The modification is mainly focused onShiftRow Transformations, if the value of 1'st element in state is even, the second and third rows are shifted right one and two times respectively, else the first and third rows are unchanged and each byte of the second and fourth rows of the state are cyclically shifted left over different number of bytes. This modification allows to remove the patterns appear.

3. Proposed Modifications

In this paper, we proposed two modifications to enhance the performance of AES algorithm to make it more compatible with ciphering of images, especially HD images. Time encryption of AES is very long, therefore we proposed decreasing the number of rounds to one instead of ten and this will lead to reduce the encryption time approximately by 1/10. The second modification we proposed new and simple S-box to reduce the computation amount as Eq. (3).

$$x(i,j) = D_1 D_2 \tag{3}$$

where $D_1 = i$, $D_2 = F - j$

where $x(i,j)$ is element value in proposed S-box with location determined by (i,j).D_1,D_2, i and j are hexadecimal numbers. The suggested S-box matrix has several properties such as, simple, generated with very low calculations, same S-box used to encryption and decryption instead of two S-box used in initial AES algorithm where this lead to reduce the ROM used by 256 byte, accordingly, reduce the hardware.

4. Experimental results

The performance of proposed method is evaluated through some factors (visible scene, histogram distribution, and correlation between adjacent pixels). Also, comparison of computation amount and encryption time between proposed method, initial AES and new version proposed in [6] is done. Experimental results clearly show that the proposed method has good result with very low encryption time in comparison with other two methods.

4.1. Visible scene and histogram

Two test images, ciphered image, histogram distribution, and correlation are shown in Figs. (1-4). Note that the histogram uniformly distributed, this means the proposed method is strong against attackers, see Figs. 2b, 4b.

4.2. Correlation

Usually, in all types of images, pixel is highly correlated with its adjusted pixels, where perfect cipher system that produces ciphered image with very low correlation between adjacent pixels [14]. One of the basic method used to measure the dissimilarity between the plain and ciphered images is a correlation coefficients technique [15]. Table 1 shows the measured correlation coefficients of the plain and ciphered images by initial AES algorithm, proposed AES version by [6], and our proposed method. Obviously that value of correlation coefficients is very low especially in modification methods proposed in [6] and our method, which means these methods are secure against various attacks. Correlation of ciphered image using our method shown in Figs. 1c-4c, where we note clearly the correlation is very low in comparison with correlation of original images.

4.3. Entropy

In image processing an entropy is defined as the measure to randomness which can be interpreted as the average uncertainty of the information source[16], [17]. An entropy is calculated by "Eq. (4)" [18]:

$$H(x) = \sum_{i=1}^{K} P(x_i)\, log_2 \frac{1}{P(x_i)} = -\sum_{i=1}^{K} P(x_i)\, log_2\, P(x_i) \quad (4)$$

where the $P(x_i)$ is the probability of symbol x_i. Now, for greyscale images the number of grey levels is 256 or 2^8 and if the probability of grey levels is equal, then by apply Eq. (4) entropy must equal to 8. The value of entropy for three samples is shown in Table 2. Results in Table 2 proved that the entropy values for our proposed methods and that proposed by [6] is very near to ideal value and best from initial AES algorithm.

Table 1.Correlation coefficients between adjacent pixels

Image	Test 1	Test 2	Test 3
Original image	0.9971	0.5902	0.9952
Initial AES	0.0362	-0.0372	0.0582
Modefied AES	0.0253	0.0097	0.0126
Our proposed method	0.0208	-0.0164	-0.0215

Table 2. Entropy values

Images	Entropy T1	Entropy T2	Entropy T3
Original image	7.3856	5.3519	7.3559
AES algorithm	7.9921	7.8333	7.9941
Modefied AES	7.9999	7.9999	7.9999
Our proposed method	7.9999	7.9999	7.9999

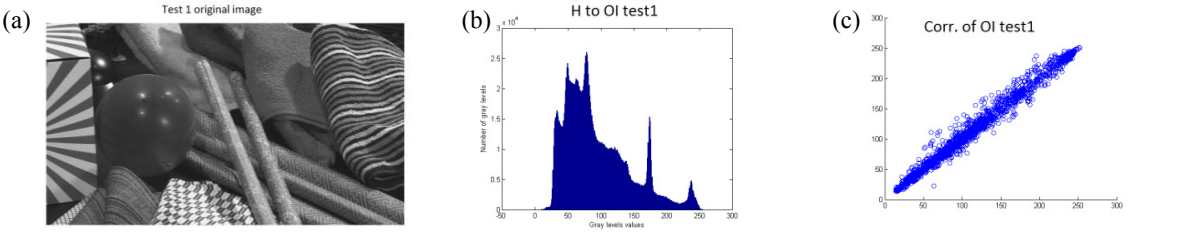

Fig. 1.original image test1 (a) OI, (b) histogram, and (c) correlation.

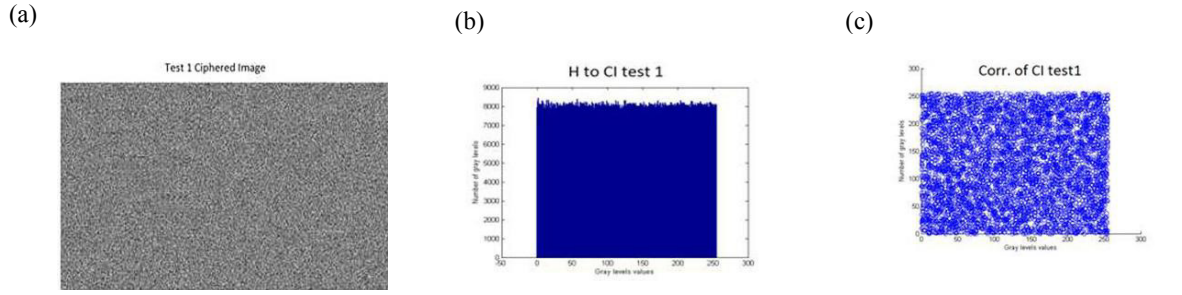

Fig.2.cipheredimage test1 with our method (a) CI, (b) histogram, and (c) correlation.

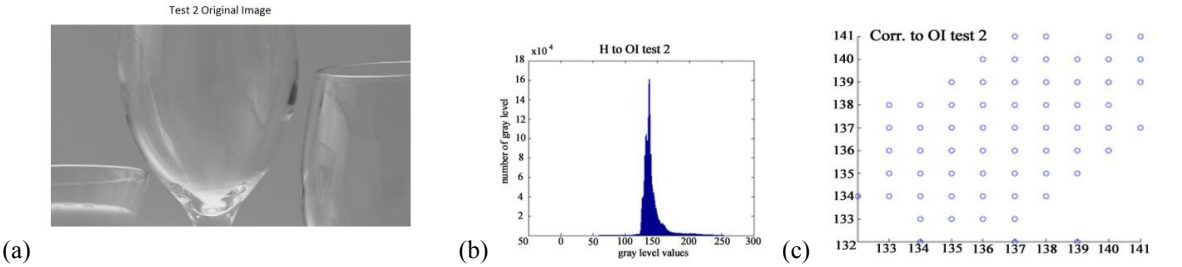

Fig.3.original image test2 (a) OI, (b) histogram, and (c) correlation.

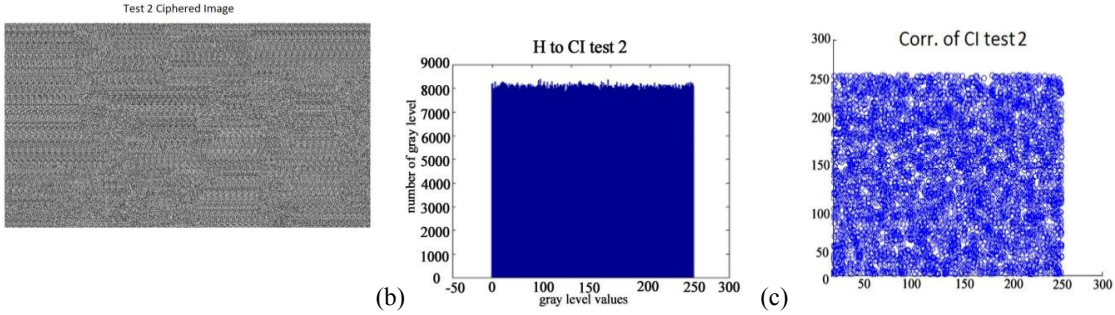

Fig. 4.cipheredimage test2 with our method (a) CI, (b) histogram, and (c) correlation.

4.4. Comparison

4.4.1. Computation comparison

The main purpose of the proposed method is to reduce the encryption time which make this algorithm compatible with HD images. In this part of experimental results, the comparison depending on the arithmetic and logic operations which executed by algorithms. Table 3 clearly shows the percentage reduction in arithmetic and logic operation in proposed modifications, where this satisfy reduction of encryption time in percentage (1/10) approximately, with the achievement of good conditions of security requirements as appear in previous parts.

4.4.2. Execution time comparison

The time required to execution of encryption and decryption operations of initial and our modified version of AES algorithm shown in Table 4 for different ciphering modes. We see that the best execution time achieved with CBC mode for both initial and modified version in encryption and decryption operations. Simulation is achieved using laptop with specifications (*HP* pavilion G4, processor Intel(R) core (TM) i5-2340M @ 2.40GHz(4CPUs),~2.4GHz, RAM 8GB, under windows 7 Home Premium 64-bit (6.1,Build 7601). From Table 4, the execution time of modified AES is reduced about 80% of the initial AES.

Table 3.Computation comparison.

	AES transformation	Arithmetic operation				
		multiplication	Addition	EX OR	Shifting	Substitution
Initial AES	S-box gen.	2048	2048	-	-	-
	Key expa.	10	-	216	10	40
	One block	288	144	160	60	160
	HD I GS(1920*1080)	37,326,858	18,664,448	20,736,216	7,776,000	20,736,056
Modified AES by [6]	S-box gen.	2048	2048	-	-	-
	Key expa.	10	-	216	10	40
	One block	288	144	160	40	200
	HD I GS (1920*1080)	37,326,858	18,664,448	20,736,216	5,184,000	25,920,070
Proposed method	S-box gen.	-	**256**	-	-	-
	Key expa.	**10**	-	**216**	**10**	**40**
	One block	**32**	**16**	**16**	**6**	**16**
	HD I GS (1920*1080)	**4,147,210**	**2,073,600**	**2,073,816**	**777,600**	**2,073,896**

Table 4. Execution time of encryption and decryption operation (in seconds).

Ciph.mod.	Modified version of AES		Initial AES algorithm	
	GS (enc. time)	GS (decr. time)	GS (enc. time)	GS (decr. time)
ECB	137.0688	142.2188	1185.8425	1189.9832
CBC	**125.4397**	**127.5297**	**1218.6240**	**1224.5419**
CFB	140.6623	144.3216	1255.6949	1263.4678
OFB	138.4400	145.4561	1286.7268	1292.4312

5. Conclusions

AES algorithm is slow because it is computationally expensive, in particular with HD image encryption. In this paper, modifications on AES algorithm are proposed to address the above-mentioned drawbacks. These modifications involved AES algorithm with one round only and using new S-box under CBC ciphering mode. Experimental results clearly show that new proposed AES algorithm makes it less computationally intensive and compatible with HD images whilefulfills the security requirements.

Acknowledgement

The authors would like to thank staff of Department of Electrical, Electronic and Systems Engineering in Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia forassisting in the completion of this work and also UKM for UKM-GUP-2011-060 andDPP-2013-001 funds.

References

[1] Wadi, S., M., Zainal, N.A low cost implementation of Advanced Encryption Standard algorithm using 8085A microprocessor. 3rd international technical conference (ITC2012),2012, pp. 157-163.
[2] Borujeni, S., E., Eshghi, M. Chaotic image encryption system using phase magnitude transformation and pixel substitution, Telecommun Syst, Springer Science and Business Media, 2011, p.13.
[3] Huang, C., W. , Yen, C., L., Chiang, C., H., Chang, K., H., Chang, C., J. The Five Modes AES Applications in Sounds and Images.6th international conference on information assurance and security, IEEE, 2010, pp. 28-31.
[4] Huang, C., W., Tu, Y., H., Yeh, H., C., Liu, S., H., Chang, C., J. Image Observation on the Modified ECB Operations in Advanced Encryption Standard.International Conference on Information Society (i-Society 2011), IEEE, 2011: p. 6.
[5] Telagarapu, P. , Biswal, B., Guntuku, V., S. Security of Image in Multimedia Applications.International Conference On Energy, Automation And Signal, IEEE, 2011, p.5.
[6] Kamali, S., H., Shakerian, R., Hedayati, M., Rahmani, M. A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption. International Conference on Electronics and Information Engineering, IEEE, 2010, 1, p. 5.
[7] Subramanyan, B., Chhabria, V., M., Sankar, T., G. Image Encryption Based On AES Key Expansion. 2nd International Conference on Emerging Applications of Information Technology", IEEE computer society, 2011, p. 4.
[8] Muhaya., Fahad, T., Chaotic and AES cryptosystem for satellite imagery. Telecommun Syst Springer Science Business Media, 2011, p. 9.
[9] Tran, M., T., Bui, D., K., Duong, A., D.Gray S-box for Advanced Encryption Standard. International Conference on Computational Intelligence and Security, IEEE computer society, 2008, p. 6.
[10] Yi-cheng, C., Zheng-lin, L., Xiao-fei, C., Yu, H. Dynamic inhomogeneous S-Boxes design for efficient AES masking mechanisms. the journal of china universities of posts and telecommunications, 2008, 15,2, pp.72-76.
[11] Jing, M., H., Chen, J., H., Chen, Z., H. Diversified Mixcolumn Transformation of AES. The 9th International Conference on Information and Communications Security", IEEE, 2008, p. 3.
[12] NIST, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 2002.
[13] Rais, M., H., Qasim., S., M. A Novel FPGA Implementation of AES-128 using Reduced Residue of Prime Numbers based S-Box. International Journal of Computer Science and Network Security, 2009, 9, 9, p. 5.
[14] Hermassi, H., Rhouma, R., Belghith, S. Improvement of an image encryption algorithm based on hyper-chaos. Telecommun Syst, Springer Science Business Media, 2011, p. 11.
[15] Fu, C. , Lin, B., Miao, Y., Liu, X., Chen, J.J. A novel chaos-based bit-level permutation scheme for digital image encryption. Optics Communications, ELSEVIER, 2011, 284, 23, p. 9.
[16] Hammad, I., M. Efficient Hardware Implementations for The Advanced Encryption Standard (AES) Algorithm. M.Sc. thesis, Dalhousie University Halifax, 2010, p. 174.
[17] Liu, P., Ding, X., Liu, D.,Sun, D. A Local Entropy based Palmprint Image Enhancement Algorithm. 1st International Conference on Information Science and Engineering, IEEE computer society, 2009, pp. 1043-1046.
[18] Gonzalez, Rafael, C., Woods, Richard, E. Digital Image Processing, Tom Robbins, New Jersey USA, 2002.